



# DISCIPLINE: Asset Management

## Discipline Roadmap for: Asset Management

Current	2 Years	5 Years	
<b>Baseline Environment</b> <b>No Baseline</b>  <u>Known products in use</u> <ul style="list-style-type: none"><li>• Microsoft System Management Server</li><li>• SAMS (Agency Management System)</li><li>• Administrative Information Management System (AIMS—old Oracle tool)</li><li>• Zenworks Asset Management</li><li>• Altiris Asset Management</li><li>• Tivoli License Manager</li><li>• Track-IT</li><li>• Access Database</li><li>• Spreadsheets</li></ul>	<b>Tactical Deployment</b> <b>Small Agency</b> ( <b>&lt;1K Clients</b> ) Database or Spreadsheet <b>Medium Agency</b> ( <b>&gt;1K and &lt;7K Clients</b> ) Altiris <b>Large Agency</b> ( <b>&gt;3K Clients</b> ) Remedy <b>Enterprise Solution</b> Remedy Enterprise  The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for IT Service Support that addresses Asset Management.	<b>Strategic Direction</b>  Market Watch  Market watch of ITIL and best practices for Asset Management.	
		<b>Shared</b> 	<b>Agency</b> 
<b>Retirement Targets</b>	<b>Mainstream Platforms</b> (must be supported)  Database, Spreadsheet, Altiris, Remedy, Microsoft SMS		
<b>Containment Targets</b>  Zenworks, Tivoli, Track-it		<b>Emerging Platforms</b>  Market Watch	
<b>Implications and Dependencies</b> Any small agency with 1K or less clients would not benefit from an asset management tool (too costly), Gartner suggests using a database or (spreadsheet). Track-IT does not have API's for integration with other systems, as all functionality is self-contained. Implications – to obtain a hardware/software inventory from an agency using Track-IT would require programming.			
<b>Roadmap Notes</b>  . Asset Management is a part of overall IT Service Management best illustrated by the IT Infrastructure Library guides, which is the most widely accepted approach to providing a comprehensive and consistent set of best practices.			

# **DISCIPLINE: Asset Management**

## **Discipline Roadmap for: Asset Management**

### ■ **Discipline Boundaries:**

- ☐ This standard applies to Asset Management tools.

### ■ **Discipline Standards:**

- ☐ All end user support tools should aid the organization in adhering to ITIL best practices for Service Delivery and Support.

### ■ **Migration Considerations:**

- ☐ Dependent on the product that data is being migrated to/from. If an API does not exist, migration could be costly. A basic knowledge of ITIL best practices will be required.

### ■ **Exception Considerations:**

- ☐ None

### ■ **Miscellaneous Notes:**

- ☐ None

### ■ **Established Date**

- ☐ November 16, 2005

### ■ **Date Last Reviewed:**

- ☐ October 25, 2006

### ■ **Next Review Date:**

- ☐ October 2007

# DISCIPLINE: Problem/Change/Configuration Management

## Discipline Roadmap for: Problem/Change/Configuration Management

Current	2 Years	5 Years	
<b>Baseline Environment</b>  Baseline on final slide	<b>Tactical Deployment</b>  The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for problem, configuration and change management. <a href="http://www.itil.com">www.itil.com</a>	<b>Strategic Direction</b>  Market watch of ITIL and best practices for problem, configuration and change management.	
		<b>Shared</b> <input checked="" type="checkbox"/>	<b>Agency</b> <input checked="" type="checkbox"/>
<b>Retirement Targets</b> Independent solutions that only address one of the above processes in a vacuum.	<b>Mainstream Platforms</b> (must be supported)  Supported OSs: Windows, AIX, Novell, Z/OS, UNIX		
<b>Containment Targets</b> DCL, LLR, and Liberium because they are not supported; products designed for DEC, Windows 2000 platforms.		<b>Emerging Platforms</b>  LINUX & Windows	
<b>Implications and Dependencies</b> Management tools must adhere to the hardware and product versions of the AOC standards. A configuration management database (CMDB) should be employed to track problem, configuration and change management.			
<b>Roadmap Notes</b> The ITIL Standards support the AOC recommendations for operating systems. Gartner cites BMC and CA as being leaders in providing solutions for ITIL compliance in problem, configuration, and change management.			

# DISCIPLINE: Problem/Change/Configuration Management

## Discipline Roadmap for: Problem/Change/Configuration Management

### ■ Discipline Boundaries:

- ❑ There should be a close interface between the Problem Management, Change Management, and Configuration Management..
- ❑ Change Management: Process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.
- ❑ Configuration Management: The process of identifying and defining Configuration Items in a system, recording and reporting the status of Configuration Items and Requests For Change, and verifying the completeness and correctness of Configuration Items.
- ❑ Problem Management:: Process that minimizes the effect on Customer(s) of defects in services and within the infrastructure, human errors and external events.

### ■ Discipline Minimum Standards:

- ❑ All tools should support the implementation of the ITIL best practice framework.
- ❑ Information Technology Information Library (ITIL) is a set of best practices used to deliver high quality IT services including problem, configuration and change management. The best practices described in ITIL represent the consensus derived from over a decade of work by thousands of IT and data processing professionals' world-wide, including hundreds of years of collective experience. Because of its depth and breadth, the ITIL has become the defacto world standard for IT best practices.

### ■ Migration Considerations:

- ❑ As with adaptation of any new business practices, training will be required.
- ❑ First, a vision has to be created. Next, the IT and business strategies should be aligned. The second step consists of analyzing the organization and its current position. In this step the organization answers the question 'where are we now?' The following step is setting goals and priorities regarding the improvement process. The fourth step is the improvement of the service through ITIL best practices in configuration, problem and change management. The fifth and final step consists of measuring the improvement to examine if processes are enhancing performance.
- ❑ Change management will require baseline analysis of IT operations processes for problem, change and configuration management.
- ❑ A basic knowledge of ITIL best practices will be required.

### ■ Exception Considerations:

- ❑ None

### ■ Miscellaneous Notes:

- ❑ Gartner reports that because of the popularity of process frameworks, such as ITIL, and the desire of IT organizations to cut costs and improve IT service and support, many IT organizations are moving beyond the vendors' traditional incident management ticketing systems to vendors that offer a richer suite of IT service support tools.

### ■ Established Date

- ❑ April 27, 2005

### ■ Date Last Updated:

- ❑ October 25, 2006

### ■ Next Review Date:

- ❑ October 2007

# DISCIPLINE: Problem/Change/Configuration Management

## Discipline Roadmap for: Problem/Change/Configuration Management

### Current Baseline Environment

ACS  
CiscoWorks  
Envision (Analysis SW)  
LAN scan  
NetBotz  
NetVision (Management Tools)  
SMP (MRTG)  
SNMP access to servers - OS tools to monitor  
ELM Performance Manager 3.0  
DS Expert 3.40  
DS Analyzer v2.02  
NetScan Pro 6.1

Cetus Storm Windows  
IBM Director  
MRTG  
Cisco WAN Mgr  
Nortel Optivity  
SNMP Utilities  
Watchguard Technologies  
Bindview RMS 7.2  
Whats Up Gold (7.4)  
HP Openview  
Somix WebNM

# DISCIPLINE: Performance Capacity Management Tools

## Discipline Roadmap for: Performance Capacity Management Tools

Current	2 Years	5 Years	
<b>Baseline Environment</b> Somix WebNM SMS-Desktop MRTG-Bandwidth (Or any MRTG/rrdtool based application) Bindview RMS 7.2 DS Analyzer v2.02	<b>Tactical Deployment</b>  The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for performance capacity management.  <a href="http://www.itil.com">www.itil.com</a>	<b>Strategic Direction</b>  Market Watch of products that enable performance and capacity management by adhering to ITIL best practices for Service Delivery and Support.	
		<b>Shared</b>	<b>Agency</b> ✓
<b>Retirement Targets</b>	<b>Mainstream Platforms</b> (must be supported)  Somix WebNM, MRTG-Bandwidth		
<b>Containment Targets</b>  SMS-Desktop, Bindview RMS 7.2, DS Analyzer v2.02		<b>Emerging Platforms</b>	
<b>Implications and Dependencies</b> – Certain open source applications are available alone or as part of a more comprehensive network management application. Because of the inherent nature of open source applications, support and training are limited.			
<b>Roadmap Notes</b> – According to Computer World Magazine, more advanced capacity planning software does more than track historical trends. It also lets IT planners create analytic models of different parts of the infrastructure to see how changes in hardware, applications or users will affect performance levels.			

# DISCIPLINE: Performance Capacity Management Tools

## Discipline Roadmap for: Performance Capacity Management Tools

### ■ Discipline Boundaries:

- ❑ SNMP based software tools providing current and historical information that indicates how well a device or service is performing and has the ability to set acceptable thresholds based on the performance information.
- ❑ **Capacity/Performance Management** tracks and manages the resources being used to satisfy the needs of the enterprise. These include storage capacity, disk space, CPU capacity, and personnel. The process also includes the creation and maintenance of a Capacity Plan.

### ■ Discipline Standards:

- ❑ All tools should support the implementation of ITIL best practices for service delivery and support.

### ■ Migration Considerations:

- ❑ A basic knowledge of ITIL best practices will be required.

### ■ Exception Considerations:

- ❑ Specialized Applications

### ■ Miscellaneous Notes:

- ❑ Forrester Research Inc. in Cambridge, Mass., states that no matter how sophisticated the analytics in the tools, the user still needs to have a thorough understanding of what parameters to model and then must interpret the data and ensure that it makes sense.

### ■ Established Date:

- ❑ November 2004

### ■ Date Last Updated:

- ❑ October 25, 2006

### ■ Next Review Date:

- ❑ October 2007

# DISCIPLINE: Network/Events Monitoring

## Discipline Roadmap for: Network/Events Monitoring

Current	2 Years	5 Years	
<b>Baseline Environment</b>  Due to the length of the list of products in the baseline, the baseline is available on the final slide.	<b>Tactical Deployment</b>  SNMP (refer to Security Domain for version)  The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for IT Service Support that addresses network events and monitoring. <a href="http://www.itil.com">www.itil.com</a>	<b>Strategic Direction</b>  Market Watch  Market watch of ITIL and best practices for network events and monitoring.	
		<b>Shared</b>	<b>Agency</b> ✓
<b>Retirement Targets</b>  N/A	<b>Mainstream Platforms</b> (must be supported)  SNMP		
<b>Containment Targets</b>  Other products in the baseline.		<b>Emerging Platforms</b>	
<b>Implications and Dependencies</b>  Network monitoring tools are dependent upon the level of successful network device management and a detailed understanding of the relationships between network components.			
<b>Roadmap Notes</b>  Standards must support state architecture’s recommendations for LAN topologies and WAN/LAN protocols. Gartner lists the following vendors as Market Leaders: ArcSight, CA, Novell, Intellitactics, NetIQ, netForensics and IBM			



# **DISCIPLINE: Network/Events Monitoring**

## **Discipline Roadmap for: Network/Events Monitoring**

### ■ **Discipline Boundaries:**

- ❑ The requirement to ascertain network problems in near real-time to ensure maximum uptime, troubleshoot problems before they impact an agency's ability to conduct business and examine historical trends for capacity planning.

### ■ **Discipline Minimum Standards:**

- ❑ Monitoring tools should ensure that data can be collected and analyzed from all devices on the network. Additionally, the need to accommodate SNMP, syslogs, and other similar data or means of data collections to develop historical and actual trends. All end user support tools should aid the organization in adhering to ITIL best practices for Service Delivery and Support.

### **Migration Considerations:**

- ❑ As with adaptation of any new business practices, training will be required on best practices and systems or applications that are new to the organization. A basic knowledge of ITIL will be required.

### ■ **Exception Considerations:**

- ❑ None

### ■ **Miscellaneous Notes:**

- ❑ None

### ■ **Established Date**

- ❑ April 27, 2005

### ■ **Date Last Updated:**

- ❑ October 25, 2006

### ■ **Next Review Date:**

- ❑ October 2007

# DISCIPLINE: Network/Events Monitoring Tools

## Current Baseline Environment

ACS  
CiscoWorks  
Envision (Analysis SW)  
LAN scan  
NetBotz  
NetVision (Management Tools)  
SMP (MRTG)  
SNMP access to servers - OS tools to monitor  
ELM Performance Manager 3.0  
DS Expert 3.40  
DS Analyzer v2.02  
NetScan Pro 6.1  
Microsoft MOM  
IPMonitor

Cetus Storm Windows  
IBM Director  
MRTG  
Cisco WAN Mgr  
Nortel Optivity  
SNMP Utilities  
Watchguard Technologies  
Bindview RMS 7.2  
Whats Up Gold (7.4)  
HP Openview  
Somix WebNM  
netForensics  
Fluke Optiview  
Cisco MARS

# DISCIPLINE: Software Distribution Tools

## Discipline Roadmap for: Software Distribution Tools

Current	2 Years	5 Years	
<b>Baseline Environment</b>	<b>Tactical Deployment</b>	<b>Strategic Direction</b>	
Novell Zenworks (SW Distribution)		→	
SMS		→	
SUS		→	
Update Expert	The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for deploying software distribution tools. <a href="http://www.itil.com">www.itil.com</a>	Market watch of ITIL and best practices for software distribution.	
		<b>Shared</b>	<b>Agency</b> ✓
<b>Retirement Targets</b> N/A	<b>Mainstream Platforms</b> (must be supported) Microsoft Systems Management Server (SMS), Novell Zenworks, SUS		
<b>Containment Targets</b> Update Expert. This product is restricted to patch management and not global software distribution.		<b>Emerging Platforms</b> Market Watch	
<b>Implications and Dependencies</b> Each agency's selection of software distribution tools will be dependant on the Network Operating System(NOS) that is deployed. We have addressed the needs of Novell and Microsoft NOS.			
<b>Roadmap Notes:</b> According to Gartner (Desktop Management Best Practices), organizations are raising the bar in terms of what they want a software distribution solution to be able to address. Companies should search for complete life cycle management suites that include imaging, software distribution, patch, usage, user data and setting migration.			

# DISCIPLINE: Software Distribution Tools

## Discipline Roadmap for: Software Distribution Tools

### ■ Discipline Boundaries:

- ❑ Policy: Policy and standardization are paramount to implementing a software distribution system. An example of a policy is restricting what users can download on their workstation computers.
- ❑ People: One of the most-critical elements of a successful desktop management strategy is staffing. The best practice is to dedicate well-trained people to managing desktops. Even if you have resources dedicated, if they do not have sufficient training on the selected desktop configuration tool success will be limited.
- ❑ Processes: Desktop configuration management processes must be defined to map to the life cycle of the PC and should include the following:
  - Initial deployment along with the development of what should be included on each initial deployment.
  - What should be included in system migrations
  - When and how often system inventories should be done
  - When and what needs to be packaged and tested before distribution
  - When and how often software updates (including patching) should be done
  - How troubleshooting and PC repair occur (for example, how long before re-imaging)
  - Moves, adds and changes, as well as incident, problem, asset and configuration management
  - Processes: Desktop configuration

### ■ Discipline Standards:

- ❑ All tools should support the implementation of ITIL best practices for service delivery and support.

### ■ Migration Considerations:

- ❑ Training should be implemented to ensure desktop configuration tool success.
- ❑ A basic knowledge of ITIL is required.

### ■ Miscellaneous Notes:

- ❑ Survey in 2006 shows SMS and Zenworks still widely used. There is also the addition of Patch Manager/Patch Link for updates on Novell systems and it runs under Windows, too.

### ■ Established Date:

- ❑ July 28, 2004

### ■ Date Last Updated:

- ❑ October 25, 2006

### ■ Next Review Date:

- ❑ October 2007

# DISCIPLINE: End User Support Tools

## Discipline Roadmap for: End User Support Tools (Help/Service Desk)

Current		2 Years		5 Years	
Baseline Environment		Tactical Deployment		Strategic Direction	
Intuit (BlueOcean) Track-IT UniPress FootPrints Epicor Clientele Front Range HEAT BMC Remedy		Minimum requirements:  The IT Infrastructure Library (ITIL) best practice framework is recommended for deployment. ITIL is the industry best practice for deploying end user support tools. <a href="http://www.itil.com">www.itil.com</a>		Market watch of ITIL and best practices for end user support.	
				Shared ✓	Agency ✓
Retirement Targets		Mainstream Platforms (must be supported) Minimum requirements: Incident management; Change management; Service level management; Remote control; Open API; Web interface; Dashboard; Escalation; Ease of use; SQL database.			
Containment Targets  Intuit (BlueOcean) Track-IT – no API's			Emerging Platforms  Market Watch		
Implications and Dependencies Recommend knowledgebase(s) to minimize problem resolution time and effort. Recommend self-service capability.  * Most important metrics - associated with customer satisfaction (# tickets per agent or other technical efficiency measures )					
Roadmap Notes Minimum standard to be reviewed annually after adoption by AOC. Gartner recognizes CA and BMC software as leaders and innovators in IT service desk solutions.					

# DISCIPLINE: End User Support Tools

## Discipline Roadmap for: End User Support Tools (Help/Service Desk)

### ■ Discipline Boundaries:

- ❑ End User Support Tools should ensure that end users are receiving the appropriate assistance. This includes the responsibility of managing all procedures related to the identification, prioritization, and resolution of end user help requests, including the monitoring, tracking, and coordination of Help/Service Desk functions. The Help Desk Manager will also contribute to problem resolution by giving in-person, hands-on support to end users at the desktop level.

### ■ Minimum Standards:

- ❑ All end user support tools should aid the organization in adhering to ITIL best practices for Service Delivery and Support.

### Migration Considerations:

- ❑ Dependent on the product that data is being migrated to/from. If an API does not exist, migration could be costly.
- ❑ A basic knowledge of ITIL will be required. Foundation training is recommended.

### ■ Exception Considerations:

- ❑ None

### ■ Miscellaneous Notes:

- ❑ None

### ■ Established Date

- ❑ September 22, 2004

### ■ Date Last Updated:

- ❑ October 25, 2006

### ■ Next Review Date:

- ❑ October 2007



# Disaster Recovery Best Practices

~~~~~

# Disaster Recovery Best Practices

## Preface

As the field of disaster recovery evolves and new expertise comes into being, new technologies and methodologies will reshape recovery strategies. Disaster Recovery Best Practices is intended to be an evolving reference and a compilation of contributions from many state agencies.

Your input on this reference is welcome. To contribute material or for questions and assistance, please contact:

Dietra Thomas  
Business Continuity Coordinator  
Division of the State CIO  
4430 Broad River Road  
Columbia, SC 29210-4012  
(803) 896-0177  
[djt@cio.sc.gov](mailto:djt@cio.sc.gov)



# Disaster Recovery Best Practices

~~~~~

## Table of Contents

	Page
Introduction.....	1
Disaster Recovery Plans .....	2
BEST PRACTICES .....	2
Risk Assessment (RA).....	3
BEST PRACTICES .....	3
Business Impact Analysis (BIA) .....	4
Recovery Class / Tier .....	5
BEST PRACTICES .....	5
Recovery Time Objective (RTO).....	6
BEST PRACTICES .....	6
Recovery Point Objective (RPO).....	7
BEST PRACTICES .....	7
Typical RTO's and RPO's.....	9
Sample Procedure to Build a Disaster Recovery Plan.....	10
Acknowledgements .....	14

# Disaster Recovery Best Practices



## Introduction

“Disaster Recovery” addresses that portion of a Business Continuity Plan which deals with the recovery of IT processing capabilities.

The measures and procedures put in place to provide disaster recovery are specific to:

- E The criticality of each processing system and its assigned RTO (Recovery Time Objective).
- E The tolerable data loss potential for that system and its assigned RPO (Recovery Point Objective).
- E The hardware, software, networking and other operating environment characteristics of the system and its dependencies.
- E The monetary and man-power resources of agencies.
- E The recovery management preferences of agencies.

These factors constitute valid and varied differences between disaster recovery strategies and can result in wide discrepancies in the disaster recovery environments designed by different agencies. However, since common components share disaster recovery considerations, agencies are urged to share their techniques and experience.

**Agencies are strongly urged to work together on their disaster recovery strategies, to pursue sharing backup and recovery facilities and resources, and to earnestly consider cooperative ventures.**

# Disaster Recovery Best Practices

## Disaster Recovery Plans

### BEST PRACTICES

- ✓ All IT facilities need documented Disaster Recovery plans.
- ✓ Copies of Disaster Recovery plans must be kept offsite and accessible to the recovery team.
- ✓ Disaster Recovery plans should be tested no less than once a year.
- ✓ Disaster Recovery plans must be maintained and should be reviewed for changes no less than once a year.
- ✓ Critical IT infrastructure requires Incident Response Plans (IRP), a type of Disaster Recovery plan specific to an infrastructure component, which specifies how to handle and recover from possible impacts that would impair that component's ability to deliver the necessary performance.
- ✓ Disaster Recovery plans must be supported by plans for all logistical support departments; such planning is contained in a Business Continuity Plan (BCP).
- ✓ Platforms which support distributed processing for one or more systems which require recovery should ideally plan for recovery at the same site. If different sites are chosen, then those sites should be sufficiently proximal to ensure the minimum throughput for each recovered system.
- ✓ If one or more related or co-dependent (front-end, back-end, etc.) IT facilities choose a given recovery site, then the other facilities sharing the co-dependency should consider choosing the same recovery site; co-dependent IT facilities should work jointly in developing their recovery strategies. Proximity not only reduces networking costs and transfer times but also reduces exposure to network disruption (fewer potential points) and recovery times.

# Disaster Recovery Best Practices

## Risk Assessment (RA)

A Risk Assessment identifies the threats to the business from natural or human-mediated (intentional or accidental) sources, rates the probability of the threats occurring, determines what impact each threat could have in consideration of the precautions and protections mounted against it, and produces a risk exposure factor for each threat, usually expressed as a probability of impact such as 1 in 10 chance of total loss, 5% probability of a power outage longer than 3 days, etc.

Risk exposures are primarily used to evaluate the degree to which a business should implement protection measures and how much investment is justified, especially for protecting structures which facilitate business processes such as buildings, power houses, network cables, communication towers, or other enabling facilities.

Risk Assessment data can be used in conjunction with the Business Impact Analysis to apply probabilities to business process outages. However, in terms of disaster recovery planning which deals with restoring IT business processes on which today's business environment is so highly dependent, it is generally accepted that IT has a zero risk exposure tolerance and so recovery planning is always required and the investment evaluation is based on the BIA alone (see "Business Impact Analysis").

### BEST PRACTICES

- ✓ A RA should be conducted for all IT enabling facilities such as data center buildings, power houses, and external communications facilities (network cables, relay stations, towers, etc.)
- ✓ Based on its RA, appropriate protection and impact mitigation measures should be implemented for each IT enabling facility.
- ✓ RAs should be reviewed for changes no less than once a year.

# Disaster Recovery Best Practices

## Business Impact Analysis (BIA)

A Business Impact Analysis (BIA) identifies each processing system's criticality, i.e. how much impact would outage of the system cause, and how long after the outage occurs would the impact be incurred. Criticality is used to plan the recovery to acceptable recovery requirements, and to determine how much should be spent on recovery capabilities, considering the following caveats or Rules Of Thumb (ROT):

**Rules Of Thumb:** (1) Technology can decrease recovery times & data loss exposure.  
(2) The faster the recovery, the more costly the technology.

Impact can be both quantitative or qualitative. Quantitative impact is usually expressed in dollars, e.g. loss of income, fines, loss of business base, etc. Qualitative impact is usually expressed as a non-numeric description, e.g. loss of lives, disruption of emergency services, damage to business reputation, loss of trained employees, missed business opportunities, etc. Impact, whether quantitative or qualitative, must be correlated with how long after the outage the impact will be incurred. Some impacts occur once at a specified time after the outage and others have recurring, and sometimes varying, impacts at various times after the outage.

The combined impact / time lapse determines the criticality of the system as illustrated in the following chart showing **Gartner's Sample Classification:**

Recovery Class/Tier	Financial Impact	Legal or Contractual	Service Impact	System Name
Multisite application	\$500,000 / day	No	Within 45 minutes	Order, Web
1	\$200,000 / day	No	Within 24 hours	Order, Internal
1	\$300,000 / day after 2 days	No	1 to 3 days	ERP
2	< \$100,000	Yes	5 to 10 days	Finance Reporting
3	None	No	Not time-critical	Data Warehouse

# Disaster Recovery Best Practices

## Business Impact Analysis (BIA) continued

### Recovery Class / Tier

Each recovery class (or tier) ranks the criticality of the system. The following basic criticality structure provides three criticality classes:

- 1 = HIGH:** the system must be recovered within a **short time**  
or **significant harm or cost** will be incurred.
- 2 = MEDIUM:** the system should be recovered within a **moderate time frame**  
or **some damage** will be incurred.
- 3 = LOW:** **little or no damage** will be incurred for an **extended period of time**.

### BEST PRACTICES

- ✓ All IT facilities need to conduct a BIA for all systems.
- ✓ BIAs are used to guide decisions on outage tolerance and how much to invest in reducing outage exposure.
- ✓ Based on these decisions, each system is assigned a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO).
- ✓ BIAs should be reviewed for changes no less than once a year.

# Disaster Recovery Best Practices

## Recovery Time Objective (RTO)

Recovery Time Objective (RTO) is the target lapse of time after a disaster by when the system should be recovered. In other words, RTO is the maximum amount of time which can elapse between the point in time when a disaster destroys the service and the point in time by which the service must be recovered or unacceptable consequences will ensue.

RTO sets a target limit on recovery time and hence is used to guide decisions in planning how recovery from a disaster will be achieved. Recovery options are limited by how much expenditure is justifiable to achieve recovery in a given time. Generally, the faster the recovery, the more expensive the solution.

Recovery investment is a business decision determined by weighing the costs of lengthening outage periods (see BIA) against the increasing expenditures needed to shorten the outage period. A realistic RTO is one which can be met by methods which fall within the recovery investment limit.

### BEST PRACTICES

- ✓ RTOs are best indicated by a Business Impact Analysis.
- ✓ A realistic RTO is one that is achievable within expenditure limits.
- ✓ All systems should be assigned a RTO, even those with low criticality.

# Disaster Recovery Best Practices

## Recovery Point Objective (RPO)

Recovery Point Objective (RPO) is the target point of recovered work. This is the state of work which will be restored to the recovered system after a disaster. Work can only be restored to the point at which it was last saved and removed to safe-keeping before the disaster.

Potential data loss is calculated by adding the times between backups and the time lapse until the backup is stowed in a safe place. It is the sum of the time since the last backup was taken and when it is safely stowed offsite.

Consider, for example, the following scenario of a “weekly” backup:

- ↓ backup1 is taken on Friday, March 5
- ↓ backup1 tapes are packaged on Monday, March 8
- ↓ backup1 boxes are stowed in the offsite vault on Tuesday, March 9
- ↓ backup2 is taken Friday night, March 12
- ↓ backup2 tapes are packaged on Monday, March 15
- ↓ disaster destroys the data center at 03:05 am Tuesday, March 16
- ↓ the only backup available for restore is backup1, taken March 5 = **11 days previous**.

If the potential data loss is more than the desired RPO, then backup and storage procedures and timing should be adjusted accordingly. In general, the lower the RPO, the more expensive the solution to achieve it. Financial considerations can increase the tolerance for a higher RPO.

### BEST PRACTICES

- ✓ The frequency of backup creation is guided by the Recovery Point Objective (RPO).
- ✓ The procedure to stow backups offsite is guided by the RPO.



# Disaster Recovery Best Practices

## Recovery Point Objective (RPO) continued

### BEST PRACTICES continued

- ✓ Backups should be stored offsite in a location which is:
  - ↓ Suitable for the physical protection of the media and its contents.
  - ↓ Secure.
  - ↓ Accessible by disaster recovery teams.
- ✓ To improve the probability of a readable copy, keep at least two full backups in offsite storage, in addition to the full backup being taken and shipped to offsite storage.
- ✓ To ensure data integrity, a media retention plan should be developed and formalized where tape media is tracked during its life cycle. Retention and re-use rates should be based on the media's reliability metrics including length of life and number of uses. The purpose of this plan is to insure that media is retired before data is lost.

# Disaster Recovery Best Practices

## Typical RTO's and RPO's

Gartner's suggested **Business Process Service Levels** :

Class	Business Process Services	Service Levels				
		Scheduled Hrs x Days	Availability		RTO	RPO
			%	Downtime		
1 * (RTE)	<ul style="list-style-type: none"> <li>Customer-/ Partner-Facing</li> <li>Functions Critical to Revenue Production</li> </ul>	24 x 7	99.9 %	< 45 mins. / month	2 hrs.	0 hrs.
2	<ul style="list-style-type: none"> <li>Less-Critical Revenue-Producing Functions</li> <li>Supply Chain</li> </ul>	24 x 6 ¾	99.5 %	< 3.5 hrs. / month	8 – 24 hrs.	4 hrs.
3	<ul style="list-style-type: none"> <li>Enterprise Back-Office Functions</li> </ul>	18 x 7	99 %	< 5.5 hrs. / month	3 days	1 day
4	<ul style="list-style-type: none"> <li>Departmental Functions</li> </ul>	24 x 6 ½	98 %	< 13.5 hrs. / month	5 days	1 day

\* Class 1 application services are those with a RTE (Real-Time Enterprise) strategy and are those that the enterprise would suffer irreparable harm from if they were unavailable.

# Disaster Recovery Best Practices

## Sample Procedure to Build a Disaster Recovery Plan

1. Perform a Risk Assessment (RA) to identify the risk exposures. See “Risk Assessment (RA)” for more information on RA.
2. Use the results of the RA to determine and implement requisite protection and precaution measures.
3. Identify every application and the IT resources required to support it.
4. Perform a Business Impact Analysis (BIA) to determine the quantitative and qualitative cost per unit of time of application outage for all the applications. See “Business Impact Analysis (BIA)” for more information on BIA.
5. Determine how much expenditure can be justified to mitigate the outage costs identified in the BIA.
6. Determine the Recovery Time Objective (RTO) for each application. See “Recovery Time Objective (RTO)” for more information on RTO.
7. Determine the Recovery Point Objective (RPO) for each application. See “Recovery Point Objective (RPO)” for more information on RPO.
8. Design (or review) a backup methodology for the application to ensure the RPO can be met. Storage vendors and storage services can present available options which include:
  - a. Performing tape backups and transporting the tapes to an offsite vault.
  - b. Managing your own offsite storage facility (vault) or contracting with a storage service provider.
  - c. Performing backups directly to offsite tape.
  - d. Using dasd mirrors to enable taking tape backups with no (or less) application downtime.
  - e. Creating synchronous or asynchronous copies on offsite dasd.

# Disaster Recovery Best Practices

## Sample Procedure to Build a Disaster Recovery Plan continued

9. Design a recovery strategy for the application to ensure the RTO can be met. Recovery site providers and recovery service providers can present available options which include:
  - a. **Hot Site** – a fully serviced facility providing the necessary environment (A/C, power, water, cabling facilities, etc.) provisioned with all required hardware which is loaded, configured and ready to go.
  - b. **Warm Site** – same as a hot site but the software (OS/applications, etc) will need to be loaded and configured.
  - c. **Cold Site** - a fully serviced facility providing the necessary environment (A/C, power, water, cabling facilities, etc.) which will need to be provisioned with the required hardware.
  - d. **Mobile Site** – an IT facility which is delivered to a pre-determined recovery site and may, or may not, house the required hardware upon delivery.
  - e. **Hot Drop or Quick Ship** – an arrangement with a provider to deliver a hardware component within a pre-arranged time much shorter than normal; these arrangements provide for priority to be given to these orders upon short notice and typically contain provisions to shorten or circumvent delays associated with the usual procurement process.
10. Document the Disaster Recovery Plan ensuring that (1) the plan will be accessible after a disaster, and (2) procedures are put in place to maintain the plan.

Note: The plan will be more current and useable (and its maintenance easier and less frequent) if titles, positions or functions are used in the main body of the plan while citing specific names only in appendices and where the documentation is person-specific, such as contact lists.

The plan documentation should include:

- a. Specific recovery procedures sufficiently detailed that they could be implemented by someone with the appropriate skill set but no knowledge of the agency or its functioning.

# Disaster Recovery Best Practices

## Sample Procedure to Build a Disaster Recovery Plan continued

10. b. An action plan detailing who is responsible for what and when, including:
  - ↓ who assesses the situation and what criteria are used,
  - ↓ who declares disaster and the procedures involved,
  - ↓ who builds the recovery environment and the procedures involved,
  - ↓ who comprises the recovery teams and who are the alternates,
  - ↓ who activates the recovery teams and the notification procedures,
  - ↓ who manages funding and other procurement needs,
  - ↓ who manages the recovery process, resolves problems and conflicts, and makes management decisions, and
  - ↓ what the reporting structure is, complete with contact numbers.
- b. All support documentation including:
  - ↓ Contracts and other legal documents.
  - ↓ Graphical summaries (maps, charts, diagrams, etc.).
  - ↓ Technical references, guides, procedures and other documentation.
  - ↓ Reference information such as directories, inventories, indices, and other 'look-up' references.
  - ↓ Pre-printed forms or other process defining tools.
  - ↓ Contact information for
    - (1) recovery team members and recovery managers,
    - (2) employees and their emergency contacts (next of kin),
    - (3) normal providers, alternate providers, and providers of recovery services,
    - (4) hardware servicing and software support,
    - (5) customers and users,
    - (6) local, county, state and federal emergency services,
    - (7) governing bodies, related agencies and other stake holders.

# Disaster Recovery Best Practices



## Sample Procedure to Build a Disaster Recovery Plan continued

11. Design and implement procedures to test the plan and apply updates. It is desirable to have different people man the tests so that as many people as possible are familiar with the details of the plan and the recovery process; this improves the likelihood of having experience available for an actual recovery.
12. Design a method for detecting and applying changes to keep the plan current. This is critical to ensuring that the plan will be effective when it is needed; constant change is a business reality, for example, consider how frequently a business must update its telephone list.
13. The entire plan should be exercised no less than once a year; portions may be exercised independently more frequently, especially to verify modifications. This process checks for changes, verifies if expectations are still realistic, and provides the opportunity to train employees and reinforce plan knowledge.
14. Monitor business changes that could impact the plan. Organizational changes may impact departmental interfaces or affect the way logistical support is provided. A location on which the plan depends on may no longer provide the expected facility. Provider agreements may change procurement plans. It is important to remain mindful of the plan dependencies and watch for any changes affecting those dependencies which could adversely impact the plan.

# Disaster Recovery Best Practices

## Acknowledgements

AOC subcommittee, Systems Management Services, January – December 2004

Doug Mader, DOR (Chair) – End-User Support

Russell Collier, DHEC – Network Events Monitoring

Debbie Dunn, CIO – Asset Management

Lee Foster, DOT – Software Distribution

Dave Gerth, CIO – Problem/Change/Configuration Management

Eric Pinckney, CIO (CIO support group liaison)

Floyd Stayner, DNR – Network Events Monitoring

Dietra Thomas, CIO – Disaster Recovery

John Ward, DOC (AOC Coordinator)

Charlie Zeberlein, CIO - Performance and Capacity Management